IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Michael A. Harclow Dustin C. Kirkland David B. Kumhyr Kylene J. Smith	Group Art Unit: 2132 Examiner: Venkatanaray Perungavoor
Serial No.: 10/713,743	Conf. No.: 2691
Filed: November 13, 2003	Atty. Dkt.: AUS920030914US1 2300.000200
For: METHOD AND APPARATUS FOR CONDUCTING A CONFIDENTIAL SEARCH	CUSTOMER NO. 46240

APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On December 6, 2007, Appellants filed a Notice of Appeal in response to a Final Office Action dated September 14, 2007, issued in connection with the above-identified application. In support of the appeal, Appellants hereby submit this Appeal Brief to the Board of Patent Appeals and Interferences.

Since the Notice of Appeal for the present invention was received and stamped by the USPTO Mailroom on December 12, 2007, the two-month date for filing this Appeal Brief is February 12, 2008. This Appeal Brief is being filed on or before the due date, therefore, it is timely filed.

If an extension of time is required to enable this paper to be timely filed and there is no separate Petition for Extension of Time filed herewith, this paper is to be construed

as also constituting a Petition for Extension of Time Under 37 CFR § 1.136(a) for a period of time sufficient to enable this document to be timely filed.

The Commissioner is authorized to deduct the fee for filing this Appeal Brief ($510.00) from IBM Corporation's Deposit Account No. 09-0447/AUS920030914US1. No other fee is believed to be due in connection with the filing of this document. However, should any fee under 37 C.F.R. §§ 1.16 to 1.21 be deemed necessary for any reason relating to this document, the Commissioner is hereby authorized to deduct said fee from IBM Corporation's Deposit Account No. 09-0447/AUS920030914US1.[1]

I. REAL PARTY IN INTEREST

The present application is owned by IBM Corporation.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences of which Appellants, Appellants' legal representative, or the Assignees are aware that will directly affect or be directly affected by or have a bearing on the decision in this appeal.

II. STATUS OF THE CLAIMS

Claims 1-20 are pending in the case, each of which was rejected as follows:

- claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over US Patent Application 2002/0174355 (***Rajasekaran)*** in view of ***Song et al***.

Appellants appeal each of the rejections. For the convenience of the Office, Appellants identify the claims in this appeal as claims 1-20.

[1] In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2300.000200.

IV. STATUS OF AMENDMENTS

After the Final Rejections, no other amendments were made to any other claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to Figure 1, a communications system 100 is illustrated in accordance with one embodiment of the present invention. As discussed in greater detail below, the communications system 100 allows users to search words (or terms) on a network (or a database) in a substantially confidential manner.

The communications system 100 includes a plurality of processor-based systems 105, 110, 120(1-3) that may be communicatively coupled by a network 130, such as by a private network or a public network (*e.g.,* the Internet). The systems 105, 110, and 120(1-3) may be any variety of processor-based systems that are capable of communicating with each other, and may include, but are not limited to, computers, portable electronic devices, Internet appliances, and the like. Although not shown, the various systems 105, 110, and 120(1-3) may be coupled to the network 130 through a router (not shown), gateway (not shown), or by other intervening, suitable devices.

In the illustrated embodiment, the system 105 includes a search module 135 that allows a user to input one or more search terms that can be provided to a search engine module 140 of the system 110. The search module 135, in one embodiment, encrypts the search term using a one-way encryption algorithm before it is transmitted to a search engine module 140, which then compares the encrypted search term to other encrypted terms accessible to the search engine. Because the search is conducted based on an encrypted search term provided by the user, as opposed to being based on the plain text

form of that search term, the user can perform the search while keeping the original search term relatively confidential.

In Figure 1, the search engine module 140 maintains a database of select words that may be found on the network 130. For example, the search engine module 140, in one embodiment, may search and maintain a database of words that are found at websites or in files associated with the various systems 120(1-3) that are coupled to the network 130. The systems 120(1-3) may be considered as various nodes on the network 130 that may have an associated website that can be searched for contents. The words found during a search and stored in the database may also contain an associated location identifying where those words can be found on the network 130. A flow diagram of how the search engine module 140 may generate a database of words is described later with reference to Figure 2. Once created, the database may be searched by the users on the network 130. The search engine module 140 may, from time to time, update the database as the contents of the various websites on the network 130 change.

In the illustrated embodiment, the systems 120(1-3) include a web server module 150, which may be capable of receiving requests over the network 130 and responding to such requests. For example, the web server module 150 may include an HTTP (Hypertext Transfer Protocol) service routine 155 that is capable of receiving HTTP requests over the network 130, as well as sending HTTP responses over the network 130. HTTP specifies how a client and server may establish a connection, how the client may request data from the server, how the server may respond to the request, and how the connection may be closed. One version of HTTP is described in RFC 2068, entitled "Hypertext Transfer Protocol—HTTP/1.1," dated January 1997. In an alternative

embodiment, the HTTPS protocol may also be employed. The systems 120(1-3) may host one or more websites that can be accessible by the search engine module 140 of the system 110. As noted, the search engine module 140 may search the websites for various words and generate a searchable database.

Figure 2 illustrates a flow diagram illustrating at least one operation performed by the search engine module 140 of Figure 1. In particular, the search engine module 140 is shown generating a database of words found on the network 130, in accordance with one embodiment of the present invention. Although not so limited, for ease of illustration, it is herein assumed that the network 130 is the Internet, and the search engine module 140 is a World Wide Web search engine. Generally, the search engine module 140 may employ software tools, sometimes referred to as "spiders," to build and maintain a database of words found on the web sites. The spider, shown as block 205 in Figure 2, accesses one or more webpages 210 on the network 130 and builds a list of words based on the contents of the webpages 210.

Those skilled in the art should appreciate that the path that the spider 205 takes in searching the Internet for words may vary from one implementation to another. In Figure 2, for example, the spider 205 uses the webpage 210 as its starting point to search for words, and then follows various hyperlinks 215 found on the webpage 210 to access other web sites. In this way, the spider 205 quickly begins to travel, spreading out across the more widely used portions of the web to build and/or update the database of words. Of course, in other embodiments, other database building and updating techniques may be employed without deviating from the spirit and scope of the present invention.

In Figure 2, when the spider 205 searches the webpage 210, it takes notes of at least two things – the words within the page, and the location where the words were found. The search engine module 140 builds (at block 225) an index of the words and their respective location. The index of words may be stored in a storage unit 230 in plain text form and/or encrypted form. In accordance with one embodiment of the present invention, the search engine module 140 encrypts (at block 235) the found words before storing them in a database 240. In the illustrated embodiment, the search engine module 140 employs the same encryption algorithm that is employed by the search module 135 (see Figure 1) to encrypt search term(s) before they are provided to the search engine module 140. The plain text form of the found words may be stored in a database 245.

Referring now to Figure 3, a flow diagram of at least one aspect of the search module 135 of Figure 1 is illustrated, in accordance with one embodiment of the present invention. The search module 135 receives (at 310) a search term from the user. The search term may be a word or a combination of words that the users desire to search on the network 130. The search module 135 encrypts (at 320) the received search term. Any one of a variety of suitable encryption methodologies can be employed to encrypt the search term. For example, the search module 135 may apply a one-way hash function on the search term, thereby making it difficult to derive the original text from the hashed string. Examples of hashing algorithms may include, but are not limited to, MD5 and SHA-1 hashing algorithms. In an alternative embodiment, an asymmetric encryption algorithm may be employed to encrypt the search term. An asymmetric encryption algorithm commonly entails mapping from message (or plain text) space to cipher space using a first key, which, for example, may be a public key. Typically, asymmetric

encryption involves a one-to-one mapping from the message space into the cipher space, where the cipher space mapping is reversible into the message space using a second key, which, for example, may be a secret or a non-public key. If asymmetric encryption is employed in the instant invention, then, in one embodiment, the search module 135 and the search engine module 140 may each have access to the public key to perform the desired encryption feature. The search module 135 provides (at 330) the encrypted search term over the network 130 to the search engine module 140.

Referring now to Figure 4, one embodiment of a flow diagram for performing a confidential search is illustrated using the search engine module 140 of Figure 1. The search engine module 140 receives (at 410) the encrypted search term that is provided by the search module 135 at block 330 of Figure 3. The search engine module 140 compares (at 420) the encrypted search term to other encrypted entries stored in the database (see element 240 of Figure 2). Based on the comparison, the search engine module 140 provides (at 330) the results to the user in plain text form. For example, if no matches are found, the search engine module 140 may indicate as such. On the other hand, if the search term matches one or more of the entries stored in the database 240, the search engine module 140 displays to the user any results that matched the search criteria.

As described above, one or more embodiments allow a user to search for a term on the network 130 (see Figure 1) without having to publicly disclose the search term. The present invention may be useful in a variety of applications where the user may desire that the search term remain a secret or where the user may wish to search for key terms without making it publicly known that the terms were being searched by the user. One application of the present invention may be illustrated with reference to an example

in which a user conceives of a word that the user believes would make a good password, and the user desires to test the strength of that password. One method of gauging the strength of the password is to check it against a large database of known words. Aside from a dictionary, the World Wide Web is another good source of a database with a large number of words. However, as described above, using a conventional search engine to search the Web may not be desirable to the user because the original password would have to be revealed to the search engine module 140, which is likely to save a copy of the searched term (*e.g.,* the password, in this example) to improve its own database. As a result of this public disclosure, the value of the secret password may be reduced, particularly if that term was not previously known on the Web.

As discussed above, one or more embodiments of the present invention allow the user to search the network 130 without having to reveal the password to the public. To conduct the confidential search, the user may utilize the search module 135 to encrypt the password before the encrypted password is provided to the search engine module 140. The search engine module 140, upon receiving the encrypted search term, attempts to match the user's encrypted password against the encrypted words stored in the database. If matches are found, they are returned to the user, indicating that the password is known to others on the Web, thereby suggesting to the user that the strength of the password is relatively weak, as it may be broken using a dictionary attack (a common scheme employed to break passwords). On the other hand, if no matches are returned, the user knows that the password does not exist in the search engine module's database, and is a relatively strong password.

Referring now to Figure 5, an exemplary webpage 505 of the search engine module 140 is illustrated through which users may search for terms on the network 130. The webpage 505, which is a Hypertext Markup Language (HTML) file, may contain one or more hyperlinks to other pages. The exemplary webpage 505 of Figure 5 may be accessed from the system 105 of Figure 1 using, for example, a web browser. For illustrative purposes, the webpage 505 is shown in a web browser window 510.

In accordance with one embodiment of the present invention, the search engine module 140 of Figure 1 allows users to search for terms in two modes – a regular mode and a secure mode. A user desiring to conduct a confidential search, may select the "secure search" option 520 using, for example, a mouse cursor 525, and then enter the search term in its encrypted form in a field 530. To initiate the search, the user may select the "begin search" button 540. The search engine module 140 may then compare the entered search term with other encrypted values of the terms stored in the database 240 (see Figure 2), and thereafter display the search results to the user.

A user may also use the webpage 505 to conduct regular (non-confidential) searches by selecting the "regular search" option 550 using the mouse cursor 525. In the regular search mode 550, the search engine module 140 performs a conventional search for the user in plain text form. The results may be displayed once the user selects the "begin search" button 540 after having entered the search criteria in the field 530. The search engine module 140 then compares the entered search term with other plain text terms stored in the database 245 (see Figure 2), and thereafter displays the search results to the user.

Against this general backdrop, the claims are discussed.

Claim 15 is directed to an apparatus for conducting a confidential search. The apparatus comprises a storage unit (650) and a control unit (615) communicatively coupled to the storage unit (650). The control unit (615) is adapted to access one or more terms associated with one or more nodes of a network (130), store the accessed one or more terms in the storage unit (650) and encrypt the stored one or more terms. The control unit (615) is further adapted to receive (410) an encrypted search term from a user, compare (420) the received encrypted search term (410) with the encrypted accessed terms and provide (430) a result of the comparison over the network (130). *See* Application, p. 8, line 16 to p. 14, line 15; Figs. 1, 3-4, 6.

Claim 1 is directed to a method for conducting a confidential search. The method comprises accessing one or more terms associated with one or more nodes of a network (130), encrypting the accessed one or more terms and receiving (410) an encrypted search term from a user. The method further comprises comparing (420) the received encrypted search term (410) with at least a portion of the encrypted accessed terms and providing (430) a result of the comparison to the user. *See* Application, p. 8, line 16 to p. 14, line 15; Figs. 1, 3-4, 6.

Claim 8 is directed to an article comprising one or more machine-readable storage media containing instructions for conducting a confidential search. The instructions, when executed, enable a processor to access one or more terms associated with one or more nodes of a network (130), encrypt the accessed one or more terms and receive (410) an encrypted search term from a user. The instructions, when executed further enable a processor to compare (420) the received encrypted search term with the encrypted

accessed terms and provide (430) a result of the comparison to the user. *See* Application, p. 8, line 16 to p. 14, line 15; Figs. 1, 3-4, 6.

Note that the reference numbers listed within the claims are provided to facilitate understanding of the claims through exemplary embodiments of the invention. As such, they are listed herein for the benefit of the Office and are not to be construed as limiting the claims in any way.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-20 are unpatentable under 35 U.S.C. 103(a) over US Patent Application 2002/0174355 (***Rajasekaran)*** in view of ***Song et al***.

VII. ARGUMENT

A. Independent claims 1, 8 and 15 (including their dependent claims) are Allowable

1. The cited references do not teach all of the claimed features

For ease of illustration, claim 15 is discussed first. Claim 15 calls for a control unit that is adapted to access one or more terms associated with one or more remote files over a network and encrypt one or more of the terms. Claim 15 further calls for the control unit to receive an encrypted search term from a user, compare the received encrypted search term with the encrypted accessed terms, and provide a result of the comparison over the network.

The Examiner relies on the combination of ***Rajasekaran*** and ***Song*** to reject claim 15 under 35 USC 103 for obviousness. Specifically, the Examiner argues that ***Rajasekaran*** discloses accessing terms over a network, and ***Song*** discloses receiving an encrypted search term and comparing it to the encrypted accessed terms. *See* Final

Office Action, p. 2. Further, the Examiner asserts that the last claimed feature of providing a result of the comparison is taught by ***Rajasekaran***. *Id.* In the Advisory Action, the Examiner reiterated the previous arguments from the Final Office Action, but stated that ***Song*** teaches outputting the search results in the Abstract and in the Theorem 4.1 and 4.2 sections.

It is well established that, to establish a *prima facie* case of obviousness, the prior art reference (or references when combined) must teach all the claimed features. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974). Moreover, each of the claimed features must be disclosed identically in the prior art. In the present case, the Examiner has failed to show that the cited references disclose each and every claimed feature identically. For example, although the Examiner asserts that ***Rajasekaran*** and ***Song*** disclose the claimed feature of "providing a result of the comparison to the user," a review of these references reveals otherwise.

The term "comparison" in this claimed feature derives its antecedent basis from the previous claimed feature, which specifies comparing the received encrypted search term with the encrypted accessed terms. ***Rajasekaran*** does not disclose such a comparison, and, therefore, cannot and does not disclose the last feature of providing a result of the comparison, as specified in claim 15. In ***Rajasekaran***, the search term (which the Examiner asserts corresponds to the "search term" in block 208) is not encrypted. *See* ***Rajasekaran***, ¶44 (describing that the unencrypted search term is compared to a decrypted "data structure"). Thus, ***Rajasekaran*** discloses providing a result based on a comparison of an unencrypted search term to a decrypted data structure, whereas the claims call for providing a result of a comparison between an encrypted

search term and encrypted accessed terms. For at least this reason, the ***Rajasekaran*** does not disclose the claimed feature of providing a result of the comparison (i.e., the comparison between two encrypted terms).

The cited passages in ***Song*** relied upon by the Examiner with respect to "providing" are silent regarding this feature. Even assuming support for *outputting* comparison results could be found in ***Song***, the Examiner's argument fails due to fundamental deficiencies in this reference**.** The term "comparison" in claim 1 can also be traced back to the "accessing" and "encrypting" features. In the instant Application, the "comparison" involves the "encrypted access terms" which are accessed and encrypted. ***Song*** does not disclose such a comparison, and, therefore, cannot and does not disclose the last feature of providing a result of the comparison, as specified in claim 15. In ***Song***, the accessed terms (*i.e.,* the data stored on Bob) are not accessed and encrypted by Bob. In fact, ***Song*** teaches that Alice, not Bob, encrypts the data to be stored on Bob. *See* ***Song***, 2: Searching for Encrypted Data, ¶2. For at least this reason, the ***Song*** does not disclose the claimed feature of providing a result of the comparison (i.e., the comparison involving encrypted accessed terms).

Claim 15 (and its dependent claims) and the other pending claims are allowable for at least these reasons. For similar reasons, claims 1 and 8 (and their respective dependent claims) are also allowable.

2. Response to Examiner's Argument

The Examiner argues that ***Rajasekaran*** teaches the last claim feature of "providing a result of the comparison." *See* First and Final Office Actions. For the Examiner's rejection to be proper, ***Rajasekaran*** must teach this feature exactly. As

explained above, however, ***Rajasekaran*** simply does not disclose providing a result of the comparison (where the comparison is between an encrypted search term and encrypted accessed terms). In fact, ***Rajasekaran*** teaches the opposite – providing results based on a comparison between an unencrypted search term and a decrypted data structure. *See* ***Rajasekaran*** ¶44 (describing that the unencrypted search term is compared to a decrypted "data structure"). The Examiner's position that ***Rajasekaran*** teaches "providing a result of the comparison" is thus belied by the reference itself.

The Examiner also argues that ***Song*** teaches the last claim feature of "providing a result of the comparison." *See* Advisory Action, Continuation Sheet (PTOL-303), ¶3. For the Examiner's rejection to be proper, ***Song*** must teach this feature exactly. However, as noted above, ***Song*** does not disclose providing a result of the comparison (where the comparison is between an encrypted search term and one or more encrypted accessed terms). In ***Song***, the server (Bob) does not access and encrypt one or more terms associated with one or more nodes of a network. To the contrary, ***Song*** teaches that the user (Alice) encrypts and then stores documents on a server (Bob). *See* ***Song***, 2: Searching for Encrypted Data, ¶2. As such, the Examiner's position that ***Song*** teaches "providing a result of the comparison" is untenable.

3. There is no reason to combine the references

Although the Examiner relies on a combination of ***Rajasekaran*** and ***Song*** to reject the claims, there is no reason for one skilled in the art to combine the teachings of these references. The Examiner asserts that ***Song*** discloses receiving an encrypted search term and comparing it against a collection of encrypted terms. In other words, according to the Examiner, the comparison is between an encrypted search term and a collection of

encrypted terms. ***Rajasekaran***, on the other hand, teaches exactly the opposite. In particular, as discussed earlier, ***Rajasekaran*** discloses receiving an unencrypted search request (at block 208) and comparing that search request against a collection of search terms ("data structure" in block 205) that are first decrypted (at block 210). One of ordinary skill in the art would not have been motivated to modify the teaching of ***Song*** since the comparison of unencrypted data would achieve the same result, namely determining whether a search had previously been performed. For at least this additional reason, the Examiner's rejection fails.

B. Claims 2, 9 and 16 are Allowable

Dependent claims 2, 9 and 16 are allowable for at least the reasons their respective independent claims are allowable, as discussed above. Moreover, these claims are allowable for additional features recited therein. For example, claim 2 specifies that the "encrypting" step of claim 1 comprises encrypting the accessed one or more terms using a same encryption algorithm as that employed to encrypt the search term.

With respect to claim 2, the Examiner argues that ***Song*** discloses "the encrypting using the same algorithm see [***Song***] (4.3 Scheme III: Support for Hidden Searches Index)." *See* Final Office Action, p. 3. This section in ***Song*** teaches that if a user does not wish to disclose the data he/she is searching for to the server holding the data, a user may "pre-encrypt" the search term. Specifically, a user employs "a deterministic encryption algorithm $E_{k''}$" and encrypts the search term W. *See* ***Song***, § 4.3, ¶2. Thus, according to the Examiner, the encryption algorithm $E_{k''}$ must be the same algorithm employed to encrypt the "accessed one or more terms" as applied to claim 1 of the instant Application. However, ***Song*** does not disclose the use of algorithm $E_{k''}$ for encryption at

any other point in the search process. Specifically, ***Song*** fails to teach the use of the $E_{k''}$ algorithm for encrypting terms accessed by the server. In contrast, claim 2 teaches encrypting the accessed one or more terms using a same encryption algorithm as that employed to encrypt the search term.

Even assuming, for the sake of argument, that the $E_{k''}$ algorithm is employed elsewhere by the user, the encryption algorithm $E_{k''}$ is not employed by the server. Because ***Song*** teaches that the user does not wish to reveal the search term to server storing the data, the server cannot employ the same encryption algorithm as the user. *See Id.* To allow the server access to the $E_{k''}$ algorithm would circumvent the utility of the user's encryption. As such, ***Song*** cannot teach encrypting accessed terms using the same encryption that was used in the received encrypted search term from the user. In contrast, claim 2, as noted, when read in light of its independent claim 1, specifies encrypting the accessed one or more terms using a same encryption algorithm as that employed to encrypt the search term. For at least the aforementioned reasons, claim 2 is allowable. For similar reasons, claims 9 and 16 are also allowable.

C. Claims 4 and 18 are Allowable

Dependent claims 4 and 18 are allowable for at least the reasons their respective independent claims are allowable, as discussed above. Moreover, these claims are allowable for additional features recited therein. For example, claim 4 specifies that the "accessing" step of claim 1 comprises accessing one or more terms contained in hypertext markup file(s) stored in one or more workstations coupled to the network. As indicated in claim 1, these accessed terms are thereafter encrypted.

With respect to claim 4, the Examiner argues that ***Rajasekaran*** discloses using "the internet and other readable formats being used." *See* Final Office Action, p. 3. Even assuming that the Examiner's assertion is true (that the reference discloses using Internet and other readable formats), such a disclosure does not teach the feature recited in claim 4. Claim 4 does not simply recite using Internet (or other readable formats). Rather, as noted, claim 4 specifies accessing one or more terms contained in hypertext markup file(s), where, as specified in claim 1, these terms are thereafter encrypted. ***Rajasekaran*** does not even mention hypertext markup files, much less how one or more terms in these files are accessed, as specified in claim 4. Although the Examiner argues that ***Rajasekaran*** discloses using "Internet or other readable formats," even the Examiner (and rightly so) does not contend that ***Rajasekaran*** discloses accessing one or more terms contained in hypertext markup file(s).

The Examiner points to paragraph 0006 of ***Rajasekaran*** in rejecting claim 4. While this paragraph makes a reference to text files and documents being in "readable, known formats," it explicitly states that these files are "not encrypted." In contrast, as noted, claim 4, when read in light of its independent claim 1, specifies encrypting one or more terms accessed from the hypertext markup file(s).

In the Advisory Action, the Examiner argues that the feature of accessing one or more terms contained in hypertext markup file(s) is taught by ***Rajasekaran*** in Fig. 4A and ¶[0007]. *See* Advisory Action, Continuation Sheet (PTOL-303), ¶2. Specifically, the Examiner argues that Fig. 4A discloses searching a set of text files and files of known formats. *Id.* An inspection of Fig. 4A, however, reveals that ***Rajasekaran*** is disclosing the partitioning of stored files based on their size. *See* ***Rajasekaran***, ¶[0066]. Fig. 4A

shows four files all having a ".doc" extension. As such, ***Rajasekaran*** teaches the partitioning of four generic documents or four Microsoft Word files (MS Word file format is denoted by a ".doc" extension). In either case, ***Rajasekaran*** is clearly not describing accessing hypertext markup file(s). ***Rajasekaran***, in ¶[0007], is completely silent regarding any kind of file formatting. This paragraph only describes the need for an efficient and secure searching technique. Thus, ***Rajasekaran*** does not teach accessing hypertext markup file(s). In contrast, claim 4 of the instant Application teaches accessing one or more terms contained in hypertext markup file(s) stored in one or more workstations coupled to the network.

For at least the aforementioned reasons, claim 4 is allowable. For similar reasons, claim 18 is allowable.

D. Claims 7, 13, and 20 are Allowable

Dependent claims 7, 13, and 20 are allowable for at least the reasons their respective independent claims are allowable, and further for the claimed features recited therein. For example, claim 20, which depends from claim 15, specifies the use of two databases (one for storing unencrypted accessed terms and the other for storing encrypted accessed terms) and further for providing a user with an option to search either of the two databases. The Examiner asserts that this feature is taught by ***Rajasekaran*** because it discloses a storage system having two memory subsystems. *See* Office Action, p. 4. Even assuming that the two memory subsystems correspond to "databases," ***Rajasekaran*** still fails to teach that these memory subsystems are for storing both encrypted and unencrypted accessed terms. Moreover, ***Rajasekaran*** does not disclose providing a user with an option to search either the first or the second database.

In the Advisory Action, the Examiner asserts the user of two databases is taught by ***Rajasekaran*** in Fig. 10, Item 1010, and by ***Song*** at 2: Searching on Encrypted Data, ¶2. Specifically, the Examiner argues that "***Rajasekaran*** discloses the *databases* for storing files." *See* Advisory Action, Continuation Sheet (PTOL-303), ¶3. However, Fig. 10 in ***Rajasekaran*** shows a single Data Store 1010. Likewise, ***Rajasekaran***, ¶¶[0123] & [0127] disclose "database 1010" and "data store 1010," respectively, Clearly ***Rajasekaran*** only teaches the use of a single database, and as such, ***Rajasekaran*** cannot teach the use of two databases and further for providing a user with an option to search either of the two databases. ***Song*** is completely silent with respect to using databases to store information. ***Song*** discloses storing files on a server (Bob). In contrast, claim 20 of the instant Application teaches this feature. For at least this reason, claim 20 is allowable. Moreover, dependent claims 7 and 13 are allowable for at least the same reasons.

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims (claims 1-20) pending in the present application over the prior art of record. The undersigned attorney may be contacted at (713) 934-4064 with respect to any questions, comments, or suggestions relating to this appeal.

Respectfully submitted,
WILLIAMS, MORGAN & AMERSON, P.C.

Date: February 12, 2008

By: /Ruben S. Bains/
Reg. No. 46,532
10333 Richmond Dr., Suite 1100
Houston, Texas 77042
(713) 934-4064
(713) 934-7011 (Facsimile)
ATTORNEY FOR APPELLANT(S)

VIII. CLAIMS APPENDIX

The claims currently under consideration, *i.e.,* claims 1-20, are listed in the Claims Appendix attached hereto.

IX. EVIDENCE APPENDIX

There is no evidence relied upon in this Appeal with respect to this section.

X. RELATED PROCEEDINGS APPENDIX

There are no related appeals and/or interferences that might affect the outcome of this proceeding.

CLAIMS APPENDIX

1. (Original) A method, comprising:

accessing one or more terms associated with one or more nodes of a network;

encrypting the accessed one or more terms;

receiving an encrypted search term from a user;

comparing the received encrypted search term with at least a portion of the encrypted accessed terms; and

providing a result of the comparison to the user.

2. (Original) The method of claim 1, wherein encrypting comprises encrypting the accessed one or more terms using a same encryption algorithm as that employed to encrypt the search term.

3. (Original) The method of claim 2, wherein encrypting comprises encrypting the accessed terms using at least one of a one-way hash function and an asymmetric encryption algorithm.

4. (Original) The method of claim 1, wherein accessing comprises accessing the one or more terms contained in one or more hypertext markup files stored in one or more workstations coupled to the network.

5. (Original) The method of claim 1, further comprises storing the encrypted accessed terms in a database and wherein comparing comprises comparing the received encrypted search term with at least a portion of the encrypted accessed terms stored in the database.

6. (Original) The method of claim 1, wherein providing the result comprises providing at least a portion of the accessed terms that substantially match the search term.

7. (Original) The method of claim 1, further comprising storing the accessed terms in a first database and storing the encrypted accessed terms in a second database, and further comprising providing the user an option to search the first database or the second database.

8. (Original) An article comprising one or more machine-readable storage media containing instructions that when executed enable a processor to:

access one or more terms associated with one or more remote files over a network;

encrypt the accessed one or more terms;

receive an encrypted search term from a user;

compare the received encrypted search term with the encrypted accessed terms; and

provide a result of the comparison to the user.

9. (Original) The article of claim 8, wherein the network is the Internet, and wherein the instructions when executed enable the processor to encrypt the accessed terms using a same algorithm utilized to encrypt the search term.

10. (Original) The article of claim 9, wherein the instructions when executed enable the processor to encrypt the accessed terms using at least one of a one-way hash function and an asymmetric algorithm.

11. (Original) The article of claim 8, wherein the instructions when executed enable the processor to store the encrypted accessed terms in a database and to compare

the received encrypted search term with at least a portion of the encrypted accessed terms stored in the database.

12. (Original) The article of claim 8, wherein the instructions when executed enable the processor to access one or more websites associated with one or more processor-based systems that are communicatively coupled to the Internet and to provide the results of at least a portion of the accessed terms that match the search term.

13. (Original) The article of claim 8, wherein the instructions when executed enable the processor to store the accessed terms in a first database, store the encrypted accessed terms in a second database, and provide the user an option to search the first database or the second database.

14. (Original) The article of claim 8, wherein the instructions when executed enable the processor to access one or more terms associated with one or more remote hypertext markup language files over a network.

15. (Original) An apparatus, comprising:

a storage unit; and

a control unit communicatively coupled to the storage unit, the control unit adapted to:

access one or more terms associated with one or more remote files over a network;

store the accessed one or more terms in the storage unit;

encrypt the stored one or more terms;

receive an encrypted search term from a user;

compare the received encrypted search term with the encrypted accessed terms; and

provide a result of the comparison over the network.

16. (Original) The apparatus of claim 15, wherein the control unit is adapted to encrypt the accessed one or more terms using a same encryption algorithm as that employed to encrypt the search term.

17. (Original) The apparatus of claim 16, wherein the control unit is adapted to encrypt the accessed terms using at least one of a one-way hash function and an asymmetric encryption algorithm.

18. (Original) The apparatus of claim 15, wherein the control unit is adapted to access the one or more terms contained in one or more hypertext markup files stored in one or more workstations coupled to the network.

19. (Original) The apparatus of claim 15, wherein the control unit is further adapted to store the encrypted accessed terms in a database and to compare the received encrypted search term with at least a portion of the encrypted accessed terms stored in the database.

20. (Original) The apparatus of claim 15, wherein the control unit is adapted to provide the result that includes at least a portion of the accessed terms that substantially match the search term, and wherein the control unit is further adapted to store the accessed terms in a first database, store the encrypted accessed terms in a second database, and provide the user an option to search the first database or the second database.